4-1-2013

Analysis of the Effects of Georgia House Bill 1113 (2008): A Case Study of the Georgia Institute of Technology's Department of Internal Auditing

Patrick A. Jenkins
Kennesaw State University

Analysis of the Effects of Georgia House Bill 1113 (2008): A Case Study of the Georgia Institute of Technology's Department of Internal Auditing

Patrick A. Jenkins

A Practicum Paper
Submitted in Partial Fulfillment of the Requirements for the

Master of Public Administration

Kennesaw State University
May 2013

Department of Political Science and International Affairs

Master of Public Administration Program

College of Humanities & Social Sciences

Kennesaw State University

Kennesaw, Georgia

Certificate of Approval

This is to certify that the Capstone Project of

Patrick A. Jenkins

Has been approved by the Program Director

For the capstone requirement for the Master of Public Administration

Professional exercise in the Department of Political Science and International Affairs

At the May 2013 graduation

Capstone Director:

David R. Shock

_____

Analysis of the Effects of Georgia House Bill 1113 (2008):
A Case Study of the Georgia Institute of Technology's Department of Internal Auditing

Executive Summary

Ethical behavior on the part of public administrators has been understood to be one of the guiding principles of public service. When public administrators decide to cross the line into behavior that is not only considered to be unethical but unlawful, they have not only put their own careers and livelihood in jeopardy, they have betrayed the public's trust. Betrayal of the public trust by state and public university employees was one of the motivating forces behind Georgia House Bill 1113 (2008). This legislation which subsequently resulted in significant changes to the University System of Georgia's policy regarding the reporting of employee malfeasance continues to have a significant impact on the internal auditing function of this state's public colleges and universities.

For this reason, the purpose of this research is to inform public administrators, particularly those working within the University System of Georgia, about the policies and standards which they are operating under. This case study of the Georgia Institute of Technology's Department of Internal Auditing reaction to Georgia House Bill 1113 will provide public administrators with a roadmap outlining how one group of public administrators has effectively accepted the challenge of maintaining the public's trust by actively combating employee malfeasance on its campus. Research findings indicate that they've not only successfully installed a fraud risk awareness and mitigation program within their audit function, but they have become a standard by which other higher education auditing departments are measured.

Analysis of the Effects of Georgia House Bill 1113 (2008):
A Case Study of the Georgia Institute of Technology's Department of Internal Auditing

Table of Contents

Acknowledgements

This research project would not have been possible without the support of several key individuals. I would like to extend my deepest gratitude to my graduate advisor, Dr. David Shock, for his guidance and supervision throughout this process. Dr. Shock's feedback and advice at critical times during this project kept it on track and helped me bring it to fruition.

I would like to thank my friend and mentor, Phil Hurd, for encouraging me to complete my studies and offer me continued support and career guidance.

I would also like to thank the staff of the Georgia Institute of Technology's Department of Internal Auditing for their cooperation and support during this project.

Finally, I would like to thank my wife, Carrie, whose devotion, support, and patience of my endeavors has enabled me to complete this life goal. I could not have done this without her.

Analysis of the Effects of Georgia 2008 House Bill 1113:
A Case Study of the Georgia Institute of Technology's Department of Internal Auditing

Introduction

Unethical behavior by public administrators and government officials rarely fails to capture headlines in the local and national media or the attention of elected officials who are in close proximity to the publicized misdeeds. Stories of corrupted public officials date back to Biblical times and even a relatively young country like the United States is not without its share of these tales. Perhaps the most notorious example would be what is known as the Watergate Scandal of the early 1970s which resulted in the collapse of President Nixon's administration, the jailing of numerous public officials, and a heightened public awareness of unethical behavior in government. In spite of numerous laws, ethics codes, and media exposure of those involved, unethical behavior by public administrators remains a challenge from Washington D.C. to the local cities and school boards.

In 2007, the State of Georgia was embroiled in a financial scandal that extended from the state's top public universities and colleges to several departments of government. The scandal originated in the discovery by state and university auditors of numerous instances of fraud involving the state's purchasing card (PCard) program. According to the University System of Georgia, the PCard program is:

> designed for the cost-effective purchase of supplies, goods, and services subject to applicable state laws, rules, and regulations to include those guidelines issued by the Georgia Department of Administrative Services (DOAS). A PCard means a charge card issued by a credit card company, bank, or other financial institution

> and provided by the State of Georgia or any of its departments or agencies under the State of Georgia Purchasing Card Program to state employees for the purpose of making small dollar purchases on behalf of such departments or agencies of the state (University System of Georgia 2010b).

At the request of then-Governor Sonny Perdue, the University System of Georgia (USG) auditors conducted an audit of USG PCard transactions for the entire 2007 fiscal year. In February of 2008, the audit report was released and found that "while the overwhelming majority of transactions reviewed were legitimate, problems with the Purchasing, or PCard, program can be traced to a lack of managerial oversight and control at every level. There were 22 cases of identified fraud, which ranged from a low of $20 to a high of $318,324, resulted in the termination of 10 employees, the resignation of 11 employees, and reprimands for five employees" (Millsaps 2008, 1). The report received both local and national attention from various media outlets.

Furthermore, the report was issued during the 2008 Georgia legislative session. In the wake of the report, a bi-partisan group of legislators in the Georgia House introduced House Bill 1113 (HB 1113), which took direct aim at issues created by the PCard scandal and addressed the use of state funds for personal gain and resulting penalties in a manner that had not been codified in state law before" (Heard, et al. 2008). The legislation was passed by the State Legislature and went into law immediately upon Governor Perdue's signature on May 14, 2008 (Georgia General Assembly 2008).

On the heels of the passage of HB 1113, Ronald B. Stark, Chief Audit Officer and Associate Vice Chancellor for the USG issued a memorandum to the Presidents, Chief Academic Officers, and Chief Business Officers and to all USG colleges and universities stating that all schools must report any and all suspected employee fraud to his office without delay (Stark 2008, 1). In addition to the new reporting requirements, the memo also stated that the Internal Audit Office for the USG would be communicating these reports of suspected employee malfeasance to the Georgia Attorney General's (AG) Office for potential criminal prosecution. Mr. Stark's memorandum on malfeasance definitions and reporting has since been formalized in the USG's Business Procedures Manual (University System of Georgia 2010a). This represented a sudden and significant change in USG policy that public administrators, from middle-management to the executive suite at all 31 USG colleges and universities, had to address.

The purpose of this project is to employ a case study approach in order to analyze of the actions of a public university after the passage of HB 1113 and subsequent USG policy changes. The objective is to provide the reader with analysis using actual examples of how public administrators have addressed and complied with general Internal Auditing industry standards for handling fraud perpetrated by employees and how they have adapted to sudden and significant changes to law and policy. The subject chosen for this case study is the Georgia Institute of Technology's Department of Internal Auditing (GT-DIA). The Georgia Institute of Technology (the Institute) is a public university which falls under the purview and administration of the USG and as such is subject to Federal and State laws, as well as, USG policies.

The new USG policy on malfeasance derived from HB 1113 represented a significant change in operational duties for college and university internal audit departments. How have the public administrators, particularly internal auditors, of the USG schools reacted to this sudden

and significant change in policy? What have they done to achieve compliance with law and policy from tactical and strategic perspectives?

HB 1113

Legislation from elected officials seeks to create or amend existing laws to meet specific challenges or needs. Often, those who draft the legislation summarize the purpose, intent or the spirit in which the law they would like passed. HB 1113's summary states that its purpose is:

> To amend Part 1 of Article 3 of Chapter 5 of Title 50 of the Official Code of Georgia Annotated, relating to general authority, duties, and procedure with regard to state purchasing, so as to prohibit the use of state funds by purchase orders, government contracts, credits cards, charge cards, or debit cards, or other such payment vehicles for personal benefit or gain; to provide definitions; to provide for the requirements of a state purchasing card program; to provide penalties for violators; to authorize the promulgation of rules and regulations; to amend Article 2 of Chapter 7 of Title 45 of the Official Code of Georgia Annotated, relating to reimbursements for public officers and employees, so as to prohibit state officers and employees from misappropriating advances of public funds, submitting fraudulent reimbursement requests, or approving fraudulent reimbursement requests; to provide for penalties; to provide for related matters; to provide for

> effective dates and applicability; to repeal conflicting laws; and for other purposes (Heard, et al. 2008).

Immediate changes called for by HB 1113 can be summarized: specific restrictions on certain items (i.e. gift cards), tighter controls on receipts from goods purchased, training and ethics requirements for PCard holders and their managers, quarterly and annual review of purchases, criminal and credit background checks for card holders, clearly defined punishment for violators and supervisors, and a "zero tolerance" policy for PCard misuse, regardless of the amount in question (Heard, et al. 2008).

USG Policy on Malfeasance Reporting

On May 6, 2008, Presidents, Chief Business Officers, and Chief Academic Officers of all USG Schools receive a memorandum from Ronald B. Stark. Mr. Stark was the Chief Audit Officer & Associate Vice Chancellor for the USG at the time. This memorandum was in regards to USG employee malfeasance and HB 1113. Critical portions of Mr. Stark's memorandum read (Stark 2008, 1):

> The recent PCard audit and associated alleged fraud has resulted in a requirement for more formalized reporting of alleged employee malfeasance to both my office and to the Attorney General's Office. Additionally, the General Assembly passed House Bill (HB) 1113 on the last day of the Session. HB 1113 also addressed aspects of PCard program management, penalties associated with PCard misuse, and the penalties associated with misuse of travel advances and fraudulent requests to the state for reimbursement. …

> Effective immediately, all USG institutions are expected to report all suspected malfeasance to my office. Currently the USG BPM Section 16.4.5 requires institutions to report malfeasance only when it has been "determined that a 'high likelihood' of impropriety greater than $1000 has occurred." However, the Attorney General's (AG's) Office has since requested that they be provided an opportunity to review all cases of alleged employee malfeasance (Stark 2008, 1).

Mr. Stark's memorandum on reporting suspected employee was later formalized into the USG's Business Procedurals Manual (BPM). Section 16.4.3 was added to clarify which college and university organizations would be responsible for the actual reporting of suspected malfeasance (University System of Georgia 2010). According to the BPM,

> The Office of Internal Audit and Compliance has the primary obligation for investigating reported malfeasance for the University System Office (USO) and for institutions without an institutional auditor. Institutional Audit departments have the primary obligation for malfeasance investigations at local campuses. The Internal Audit departments at both the Board level and the institutional level may contact other departments, including the Legal Office and university police departments, to establish the necessary team to proceed with the review or investigation (University System of Georgia 2010).

USG policy is clear in stating that the responsibility for reporting employee malfeasance lies with the campus' Internal Audit departments.

Literature Review

Literature for this case study was collected through information obtained from various sources. The literature was gathered from areas that are more general in nature, such as standards and certifications put forth by the internal auditing and fraud investigation industries. This literature was combined with public records maintained by the State of Georgia, the USG and GT, as well as, interviews with key personnel.

Industry Certifications and Standards

As stated in the introduction, the new USG policy mandates that the Internal Auditing function of each school will be directly responsible for reporting employee fraud or malfeasance. This calls into question the capabilities, training and education of those employed within each school's internal auditing function. As all public administrators do not fit the same mold in their job responsibilities, neither do all USG auditors. Industry competency can be expressed through the attainment of certifications by the auditor and there are several organizations which provide certifications based on the auditor's area of expertise. It can be said that the traditional concept of an auditor is that of a professional whose background is one of financial proficiency and is commonly associated auditing the tax returns of citizens under the guidance of the Internal Revenue Service (IRS). While the traditional accounting auditors made famous (or infamous) by the IRS are still a significant portion of the industry, other areas of auditing expertise have been on the rise for the last several decades. The Institute of Internal Auditors (IIA), for example, offers the official recognition of the Certified Internal Auditor® (CIA) certification. According

to their literature, a CIA candidate must be able to pass pre-qualification screening, which includes the completion of a four-year degree from an accredited college or university, over two years of experience working within the auditing industry, and a character reference signed by an existing certificate holder (The IIA 2013). Once pre-qualifications have been met, the candidate must be able to pass a four-part exam covering governance and auditing principles, adherence to ethics standards, and certification maintenance through continued professional education (The IIA 2013). Based on this information, only educated and experienced individuals will qualify to hold this certification. According to an IIA press release in 2011, there are over 100 thousand CIA's world-wide (The IIA 2011).

Auditors whose job functions require them to focus more on technology rather than finance might pursue the Certified Information Systems Auditor (CISA) certification issued by the Information Systems Audit and Control Association (ISACA). As with the CIA certification, CISA candidates must have four-year degree from an accredited college or university and at least three years of security, information systems, or auditing experience and pass a rigorous written exam (ISACA 2013). Unlike the CIA, however, CISA candidates are eligible to take the certification exam prior to meeting the education eligibility requirements. However, even if they pass the exam, they are not considered CISAs until all qualifications have been satisfied. CISAs are also required to maintain their certification through continued professional education and must attain at least 120 hours of continued education over a period of three years and adhere to the organization's ethics standards (ISACA 2013). As with the CIA, CISAs are highly educated and experience individuals who maintain their certifications through practice and education.

Those auditors who are tasked with auditing specifically for fraud would probably consider obtaining the Certified Fraud Examiner (CFE) credentials issued by the Association of Certified Fraud Examiners (ACFE). Unlike the CIA and CISA, the CFE candidate must acquire a certain amount of ACFE points to qualify. While a college degree does substantially increase the candidate's point score, unlike the CIA or CISA, it is not a requirement. The ACFE also places great value in the candidate's experience, as well as, their ability to pass a written exam (ACFE 2013). As with other certifications, continued professional education is mandatory.

Of course, there is the traditional standard for most banking and financial professionals, which is the Certified Public Accountant (CPA). According to literature on the American Institute of CPAs (AICPA), candidates seeking the CPA certification must have at least 150 semester hours of college education and pass a comprehensive written exam. Furthermore, unlike the CIA, CISA, and CFE which are global certifications, the CPA is licensed under a particular state's Board of Accountancy (AICPA 2013).

While there are several other industry certifications which focus further on specific skills, the above-mentioned certifications should be accepted as the most common. It is also not uncommon for auditors to hold one or more industry accepted certifications. This is also not uncommon amongst auditors in leadership positions who must be prepared to evaluate controls across multiple disciplines. Even though certifications address specific auditor competencies and education, the guiding principles for internal auditing industry are the "Standards for the Professional Practice of Internal Auditing" which are published by the Institute of Internal Auditors (IIA) (The Institute of Internal Auditors 1997). These standards are comprehensive and provide the framework and criteria by which internal auditing groups are expected to operate.

Section 280 of the Standards speaks to the internal auditor's responsibilities in the matters of fraud within their organization. Section 280.02 states, "Internal auditors are not expected to have knowledge equivalent to that of a person whose primary responsibility is detecting and investigating fraud" (The Institute of Internal Auditors 1997, 25). However, that same section clarifies that internal auditors are to "have sufficient knowledge of fraud to be able to identify indicators that fraud may have been committed … be alert to opportunities, such as control weaknesses that could allow fraud … and to notify the appropriate authorities within the organization if a determination is made that there are sufficient indicators of the commission of a fraud to recommend an investigation" (The Institute of Internal Auditors 1997, 25).

At this is point it has been established that internal auditors should be aware of industry guidance and education, as well as, adhere to their industry's operational standards which include a basic ability to identify and report on fraud within their organization. To focus in on the details of this case study, specific and relevant literature must be examined.

Employee Malfeasance

It is important to understand the spirit of the time in which HB 1113 and the USG Policy on Reporting Employee Malfeasance came to fruition. In addition to release of the USG Audit Report on PCards, press releases by the Georgia Attorney General's Office and reports from print and television media during the spring of 2008 were exposing higher education public administrators' abuse of the public trust through their fraudulent actions. Two of the most egregious examples were those of Michelle Harris and Donna Gamble:

- Michelle Harris

  According to a press release by Georgia Attorney General Thurbert Baker, while Ms.

Harris was employed at Georgia Tech's College of Management, she was issued a PCard, which she misused for personal gain. Harris used her PCard pay for many personal items, including her wedding cake, and other personal expenses totaling $173,186.46 over a period of several years (Baker 2008). Ms. Harris eventually pled guilty to racketeering in 2009 and was sentenced to 10 years in jail and 10 years probation (Siegel 2011, 235).

- Donna Gamble

  According to an Atlanta Business Chronicle article, Ms. Gamble was employed by Georgia Tech in the Institute for Bioengineering and Bioscience. During her employment she used her Georgia Tech PCards to make over 3,800 transactions for personal items, at a total cost of more than $316,000 (Atlanta Business Chronicle 2008). In an effort to conceal her crimes, she forged payment receipts and her supervisor's signature and also manipulated the accounting records (Atlanta Business Chronicle 2008). Ms. Gamble pled guilty to 22 counts of mail fraud in Federal Court and was sent to Federal prison (Atlanta Business Chronicle 2008).

While Ms. Harris and Ms. Gamble represented the largest amounts of higher education employee malfeasance during the spring of 2008, they were certainly not alone. They were joined by several other university employees making the news over their malfeasance:

- Wanda Wilson

  According to Atlanta WSB News, Wilson, a former employee Georgia Tech's School of Electrical and Computer Engineering was arrested and ultimately pled guilty to "two counts of theft by taking. The GBI says she used her state issued purchasing card for a

laptop computer, a web cam and Internet chat headset. The total value was $724" (WSBTV 2008).

- Angela Young

  Atlanta WSB News reported that Angela Young, a Georgia Tech employee in the College of Computing was arrested in March of 2008 and charged with eight felony counts of theft by taking. The GBI reports stated that she used her PCard to illegally purchase $936.92 cable television and pay-per-view videos at her residence (WSBTV 2008).

- Jana Chambers

  Atlanta WBS News also reported that Jana Chambers, a former Georgia Tech employee was arrested on March 19 [2008] and was charged with six counts of felony theft by taking. According to the GBI, Ms. Chambers used her PCard to purchase personal DVD's and make-up valued at $604.02 (WSBTV 2008).

Certainly these few people do not represent the thousands of honest public administrators within GT. However, the betrayal of public trust by a few employees and the subsequent media coverage of these facts during the spring of 2008 almost certainly affected the decisions by Georgia lawmakers and USG leadership to make sweeping changes in laws and policy related to public employee malfeasance.

Malfeasance Defined

In addition to adding reporting requirements on the discovery of fraud being committed by USG employees, the new policy further defined employee malfeasance, which until 2008 had loose interpretations at the various USG schools. This is not surprising since the existing policy had gaps and was subject to each school's own interpretation. This idea is also consistent with

some of the basic concepts of public administration theory. In the book Public Administration: Social Change and Adaptive Management authors Cayer and Weschler point out "subunits may diverge in their pursuit of organizational goals. Subunits develop their own norms and ways of doing things that may not be consistent with the needs of the organization as a whole. The resulting dissonance may impede the rational pursuit of the overall goal" (Cayer and Weschler 2003, 16-17). This certainly appears to be the case with the 31 schools of the USG and how each school may have defined malfeasance.

The new USG definition of malfeasance states, "employee malfeasance generally include instances of embezzlement, misappropriation, alteration or falsification of documents, false claims, theft of any asset, inappropriate use of computer systems to include hacking and software piracy, bribery or kickback, etc." (Stark 2008, 2). This broader definition of employee malfeasance also provided with USG public administrators with new and different challenges to address. However, the goal of removing ambiguity from definitions and scope of employee malfeasance was achieved.

Malfeasance Reporting Responsibilities

As stated earlier, USG policy on malfeasance reporting mandates that, "institutional Audit departments have the primary obligation for malfeasance investigations at local campuses" (University System of Georgia 2010). Unlike many other schools within the USG, GT has their own audit department with multiple auditing divisions. After review of industry requirements and expectations regarding auditor competencies and their ability to identify fraud, it is clear that the USG policy on malfeasance (or fraud) reporting is well within the defined standards for the internal auditing industry.

Methodology

The methodology for this project is an exploratory case study of the internal auditing departments of GT. The 2008 PCard Audit Report released by USG outlined 22 cases of "notable violations and fraud" and of these 22 cases, 12 cases occurred at GT (USG Office of Internal Audit 2008). Ethical considerations for this include using only information that is available via public record and excluded any information that could impede or hinder current employee malfeasance investigations.

Case Study

The study looked at how GT-DIA existed prior to the PCard scandal and HB 1113 and how it has adapted to the subsequent policy changes from 2007 to 2013. This includes the collection and qualitative analysis of data related to the departments' budgets, organizational structures, internal policies and procedures, staffing decisions, training curriculum, and tools acquisitions specific to the internal audit function. Data was obtained through intensive interviews with key personnel (see Appendix A), as well as, requests for public records under the Georgia Open Records Act. The data was broken down into six key sections for review:

1. Department Activities
2. Staffing and Industry Certifications
3. Department Budget
4. Employee Training
5. Tools and Resources
6. External Assessment

The data collected has been analyzed and compared to see if and how the public administrators in GT-DIA have allocated resources to achieve compliance with USG policy, audit industry standards, and state law. The method of data collection for this was approved by Kennesaw State University's Institutional Review Board on February 8, 2013. Interviews and records review with key GT-DIA personnel took place on March 18, 2013 in their office at Georgia Tech in Atlanta, GA.

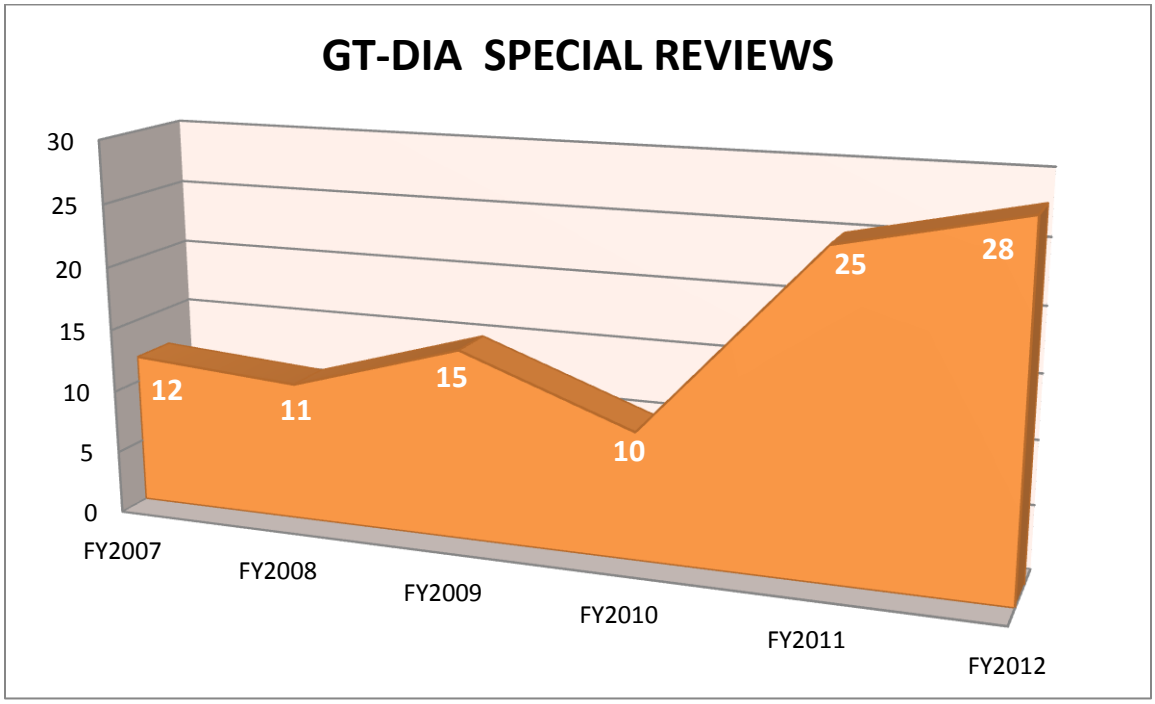
Findings

The findings for this case study indicate that GT-DIA was affected by HB 1113 and changes to USG Policy. The ripple effects of the policy change appear throughout the department. While many departments undergo change due to routine circumstances, such as employee turnover, new leadership, or fiscal restructuring, GT-DIA's activities, capabilities, financial requirements, training, and resources are very different today than in 2007.

1. *Department Activities*

GT-DIA's operations and activities consist of regular, planned audit engagements with various Georgia Tech schools and departments, which are standard operating procedure for most internal auditing functions. These activities are classified as "Departmental Reviews". However, audit activities that involve suspected employee malfeasance are categorized as "Special Reviews" and are assigned with coding label identifying them as such (Auditing 2013). According to GT-DIA records and interviews, GT-DIA has seen a significant increase in Special Reviews reported over the past years. This indicates that GT-DIA has been complying with USG requirements on reporting suspected employee malfeasance. Illustration 1.1 shows the increase of GT-DIA Special Reviews since 2007 (Auditing 2013):

Illustration 1.1 – GT-DIA Special Reviews



Source: Auditing 2013

According to their information and records, GT-DIA's Special Review cases involving suspected employee malfeasance has increase from twelve cases in FY2007 to twenty-eight cases in FY2012 (Note, FY2013 is still underway as of this publication). This represents an increase of over 133% in cases alone and according to the GT-DIA Director, these numbers directly attributable to HB 1113 and the subsequent USG employee malfeasance reporting requirements (Auditing 2013).

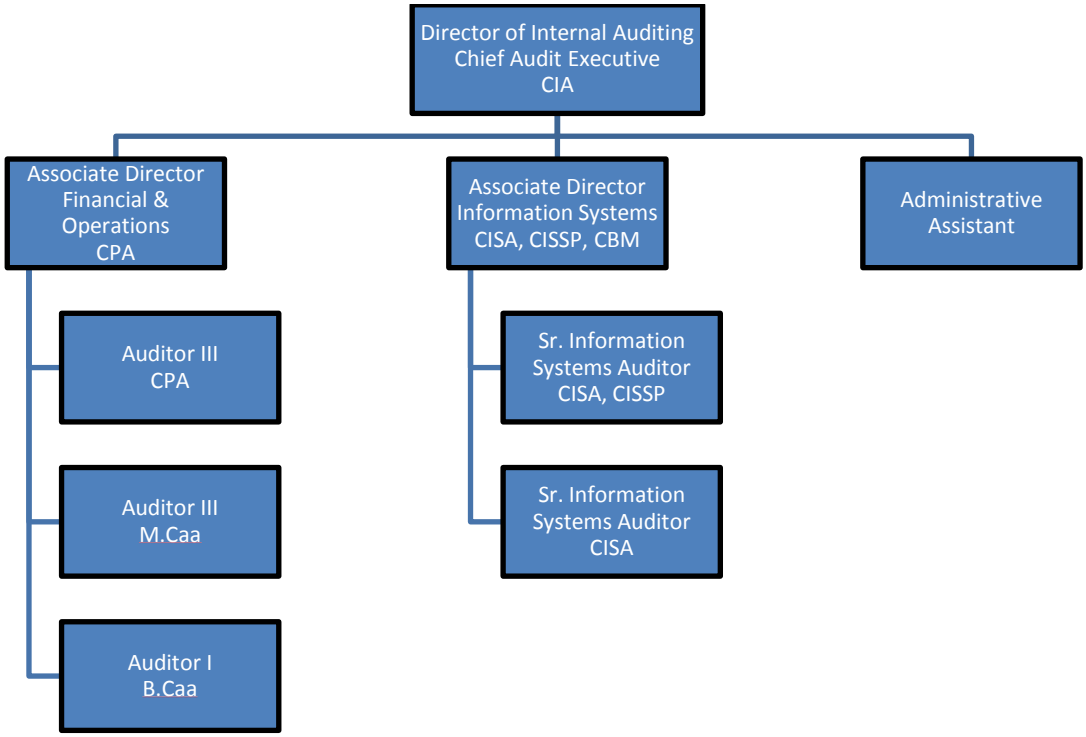
HB 1113 also brought other changes to GT-DIA activities, as well. According to the GT-DIA Director, "Prior to HB 1113, judgment on employee issues was kept as a local decision or choice by university management. Leadership decisioning was replaced by legal precedent for action. In addition to suspected employee malfeasance we now had to assess manager

culpability in the suspected malfeasance. This resulted in a dramatic increase in the need for fraud detection capabilities including a fraud risk assessment program. We've also added a fraud awareness element to our standard audit program called Departmental Reviews" (Auditing 2013).

2. Staffing and Industry Certifications

The change in activity related to HB 1113 also resulted in substantial staffing changes within GT-DIA. In 2007, staffing levels included nine (9) full-time employees (FTEs), eight of which were dedicated to audit functions. The organization was headed by the Chief Audit Executive and was sub-divided into two groups: Operational and Financial Audits and Information Systems Audits. Each group was managed by an Associate Director and each auditor held, at a minimum, a Bachelor's degree. Most auditors held advance degrees and industry certifications. See Illustration 1.1 for more details on GT-DIA's staffing and certifications in 2007.

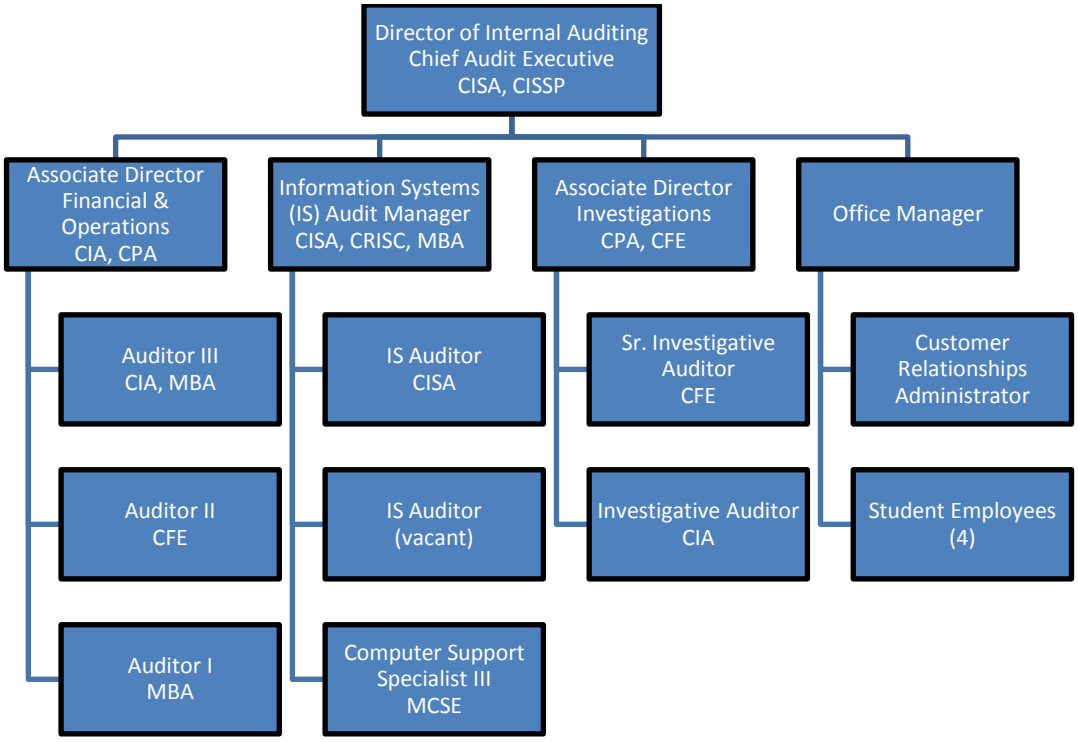
Illustration 2.1 – GT-DIA Organization in 2007



Source: Auditing 2013

By 2013, GT-DIA's organization had changed significantly. In addition to a new Chief Audit Executive, the organization has reorganized with a greater focus on fraud auditing and detection. This is evident in the additional FTEs, including an Associate Director for Investigations, as well as, the increased levels of industry certifications. In 2007, GT-DIA did not have an auditor on staff with a CFE certification. As of 2013, three members of their staff hold the CFE certification [see Illustration 1.2 for more details on staffing changes and certifications].

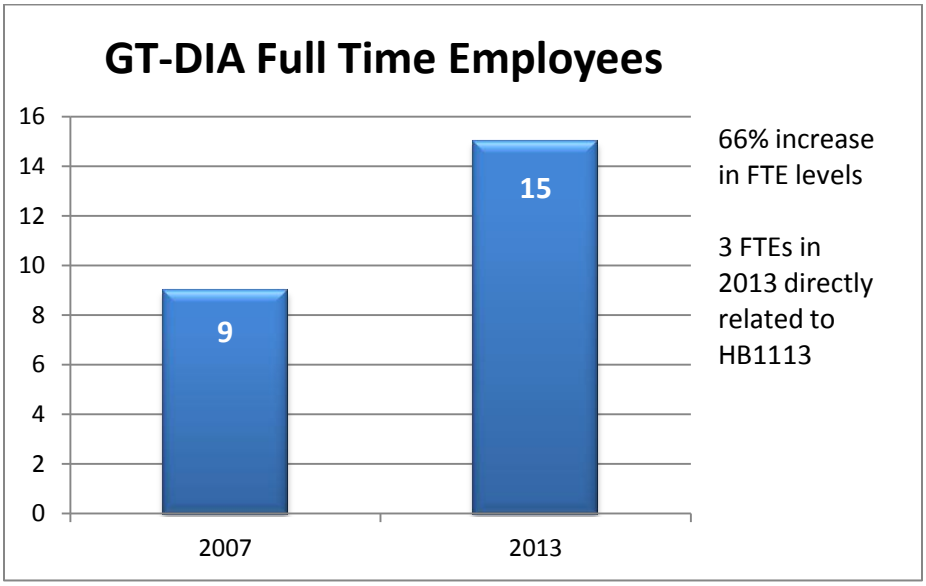
Illustration 2.2 – GT-DIA Organization in 2013



Source: Auditing 2013

As of 2013, GT-DIA has filled thirteen FTE positions. In addition to the FTEs, they currently employ four Georgia Tech student employees and have plans to expand the student employee program in the future. According to staffing time allocations, student employees are counted as half of FTE. Therefore, four student employees are counted as two FTEs for employment head counting statistics. This brings GT-DIA's 2013 staffing head count to a total of fifteen FTEs, compared to nine in 2007. This represents a 66% increase in staffing for GT-DIA.

Illustration 2.3 – GT-DIA FTE Staffing Levels



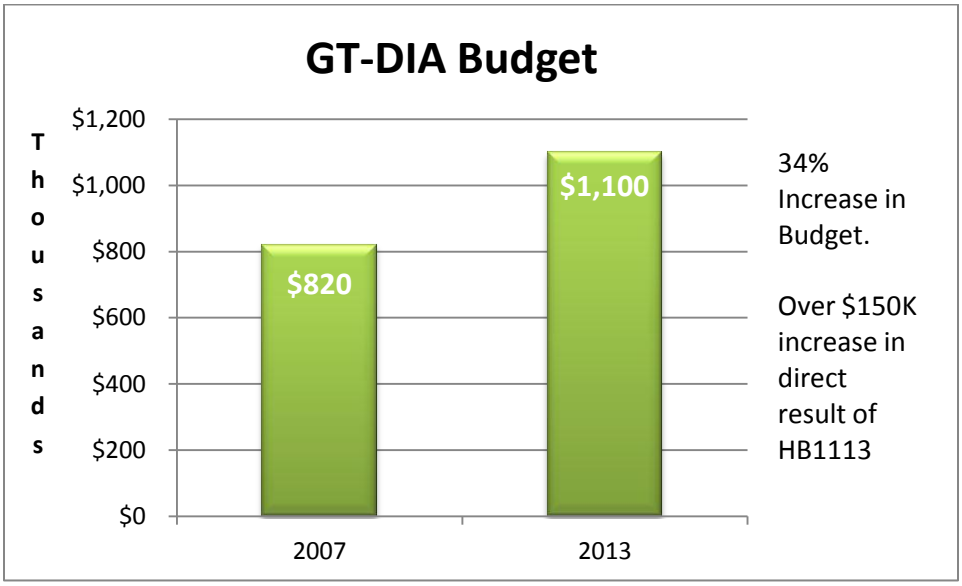
Source: Auditing 2013

According to information provided by the GT-DIA Director, at least three of the FTE positions (50% of the FTE increase) are directly attributable to HB 1113 and the subsequent USG employee malfeasance reporting requirements (Auditing 2013). This data shows that GT-DIA has expanded their staff and industry certifications to address the need of being able to properly identify suspected employee malfeasance, as prescribed by USG policy.

3. Department Budget

Along with staffing increases, GT-DIA experienced budget increases during this time period, as well. According to GT-DIA records, in 2007, the department's budget was at $820 Thousand. As of 2013, the budget stands at over $1.1 million. This is an increase of over $280 Thousand (34%) during that time period.

Illustration 3.1 – GT-DIA Budget Levels



Source: Auditing 2013

According to information provided by the GT-DIA Director, at least $150,000 of the $280,000 budget increase during that time period (53% of the budget increase) is directly attributable to HB 1113 and subsequent USG employee malfeasance reporting requirements (Auditing 2013). This data indicates that GT-DIA has received funding increases from Georgia Tech to specifically address reporting and investigative capabilities on suspected employee malfeasance.

4. *Employee Training*

As seen under the increase in staffing, GT-DIA has experienced an increase in industry certifications and training since 2007. According to the GT-DIA Director, the department policy has always included regular employee training and industry certification. He stated further that, "After HB 1113 we had the need to include CFE and forensics certifications to our inventory. As of now we have three CFEs in the office, two of which are assigned directly to the

investigative team. One of those FTEs is currently pursuing a GIAC Certified Forensics Analyst (GCFA) certification to expand our abilities in the areas of computer forensics and data analysis" (Auditing 2013). The Director elaborated further that GT-DIA auditors are in the process of migrating to more adaptive skill set and that given the exposure employee malfeasance at the university that all auditors have a basic knowledge of fraud detection and identification (Auditing 2013). As a result of this, one of the GT-DIA auditors assigned to audit the automated continuous monitoring tool for the university's PCard system of record has obtained a CFE certification, as well (Auditing 2013).

Furthermore, all GT-DIA auditors are expected to be actively engaged in their respective industry organizations. According to the current President of the Association of College and University Auditors (ACUA), GT-DIA plays an active role in the organization by serving on organizational committees, teaching classes as subject matter experts, and coordinating events at the organization's annual conferences (Auditing 2013). This information shows that GT-DIA has placed employee training related to identifying and reporting on employee malfeasance as a prior within their department.

5. *Tools and Resources*

In addition to staffing, budgetary, and employee training increases, GT-DIA auditors have also experienced an increase in other resources and tools since 2007, many of which are used to detect employee malfeasance. These tools have been deployed at the enterprise-level and at the local department level. According to the GT-DIA Director, "We have advised the university on implementing automated data analytics tools and platforms to provide more oversight of various financial systems. These tools have enabled management and Internal Auditing to be more responsive to anomalies which could represent fraudulent activity. As the

Institute has been receiving more Federal agency oversight, these tools have also been very useful in providing them pertinent information on a timely basis" (Auditing 2013).

GT-DIA also manages the university's ethics hotline and has engaged in promotional and customer relations engagements to advertise the service (Auditing 2013). Illustration 5.1 show an example of a postcard which was mailed to all Georgia Tech employees.

Illustration 5.1 – GT-DIA Ethics Hotline Awareness Post Card

According to the GT-DIA Director, in addition to the post cards, "we've also used other communication outlets, such as postcard mailings, pens, and various promotional and targeted items to advertise the Institute's ethics hotline. We believe that these efforts will discourage

"fraud opportunists" from committing unethical actions they may have otherwise committed without the proper awareness" (Auditing 2013).

At the departmental level, GT-DIA has invested in technology which has enabled them to meet the need of integrating with Federal and State law enforcement during Special Reviews where law enforcement assistance has been necessary (Auditing 2013). Furthermore, the department has invested in a high-end computer workstation with advanced multimedia hardware and software to generate training materials, including curriculum for fraud risk identification and ethics training (Auditing 2013). According to the GT-DIA Director, the ethics hotline, fraud detection tools, and awareness campaigns are all directly and indirectly attributable to HB 1113 and subsequent USG employee malfeasance reporting requirements (Auditing 2013). This data indicates that GT-DIA and Georgia Tech have invested in proper resources and tools to not only detect employee malfeasance, but to educate the campus in an effort to deter fraudulent behavior.

6. External Assessment

GT-DIA has also been reviewed and commented on by its peers in the auditing industry and from executives with the State of Georgia's Government. According to its policy, GT-DIA must undergo a period peer evaluation called an External Quality Assessment (EQA) (Auditing 2013). This is to ensure compliance with the Quality Assurance requirements outlined in Section 560 of the IIA Standards (The Institute of Internal Auditors 1997, 80). GT-DIA's most recent EQA was performed in 2012 and the executive summary of the subsequent report outlined the peer perception of GT-DIA's operations. The external auditors conducting the EQA, Ms. Betsy Bowers, Mr. William Mulcahy, and Mr. Gottesman stated,

> GT DIA is known as the 'go to' internal audit operation among its higher education peers. This office is seen as a leader in Information Technology (IT), forensic, PCard, and departmental auditing. Internal Audit has also been a catalyst for the establishment and upcoming launch of the Institute's control self assessment. Recently, a Forensic Audit unit was established in DIA. We note, however, that these activities have undermined the full cadre of services DIA may provide GT. Currently, Institute perception of DIA is of being exclusively campus investigators instead of the more helpful reputation of assurance specialists and consultants. During the upcoming year, we believe the DIA will be recognized for their assurance and consulting activities because of the strategic vision of the Director/Chief Audit Executive (CAE) of the DIA (Bowers, Mulcahy and Gottesman 2012, 4).

In addition to their auditing industry peers, GT-DIA's efforts on investigating employee malfeasance have garnered the respect from state officials in law enforcement. According to a news report in 2011 regarding a Georgia Tech Professor who had allegedly engaged in fraudulent activity, the question arose of why Georgia Tech seems to be in the news regarding employee malfeasance? During the interview with the news report, Georgia Senior Assistant Attorney General David McLaughlin praised GT-DIA for their diligence. He stated that, "it may seem like Georgia Tech has a lot of these cases, but it could just be that the school is better at catching wrongdoing and reporting it" (WSB TV 2011). It appears that GT-DIA's reputation as subject matter experts on detecting and reporting employee malfeasance has been a result of their

efforts in complying with the aftermath of HB 1113.

Conclusions

The evidence collected indicates that HB 1113 and subsequent USG policy changes have had a profound impact on Georgia Tech and its Department of Internal Auditing. It is also clear that GT-DIA and the public administrators in that department have adjusted to meet the new requirements under the law and policy. These adjustments to their activities, staffing, budgeting, employee training, expanded resources and tools have not only enabled them to comply with USG reporting requirements, but according to their peers, they have become the higher education example for investigating and reporting on employee malfeasance. Based on the evidence reviewed in the case study, the data suggests that the public administrators of GT-DIA have successfully and comprehensively adjusted to the significant USG policy changes resulting from HB 1113.

References

ACFE. 2013. CFE Qualifications. http://www.acfe.com/cfe-qualifications.aspx [Accessed February 27, 2013].

AICPA. 2013. FAQs - Become a CPA. http://www.aicpa.org/BecomeACPA/FAQs/Pages/FAQs.aspx [Accessed February 17, 2013].

Atlanta Business Chronicle. 2008. Former Georgia Tech worker gets jail time for mail fraud. http://www.bizjournals.com/atlanta/stories/2008/08/18/daily29.html [Accessed February 1, 2013].

Auditing, GT Director of Internal. Interview by Patrick A. Jenkins. Personal interview. Atlanta, March 18, 2013.

Baker, Thurbert E. 2008. Attorney General Baker Indicts Former Georgia Tech Employee in Massive Purchasing Card Abuse Case, Attorney General of Georgia Press Releases. http://law.ga.gov/press-releases/2008-03-24/attorney-general-baker-indicts-former-georgia-tech-employee-massive [Accessed February 1, 2013].

Bowers, Betsy, William Mulcahy, and Robert Gottesman. 2012. Quality Assessment Report. *Georgia Tech Internal Audit External Quality Assessment*. Atlanta, GA: IIA.

Cayer, N. Joseph, and Louis F. Weschler. 2003. *Public Administration: Social Change & Adaptive Management, 2nd Edition.* San Diego, CA: Birkdale Publishers.

Georgia General Assembly. 2008. 2007-2008 Regular Session - HB 1113. http://www.legis.ga.gov/Legislation/en-US/display/20072008/HB/1113 [Accessed February 1, 2013].

Heard, John, Ed Rynders, Penny Houston, Greg Morris, and Richard Royal. 2008. "House Bill 1113 (AS PASSED HOUSE AND SENATE)." Georgia General Assembly. http://www.legis.ga.gov/Legislation/en-US/display/20072008/HB/1113 [Accessed February 10, 2013].

ISACA. 2013. How to Become CISA Certified. http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/How-to-Become-Certified/Pages/default.aspx [Accessed February 27, 2013].

Millsaps, John. 2008. USG Releases P-Card Audit Report, USG Newsroom. http://www.usg.edu/news/release/usg_releases_p-card_audit_report [Accessed October 10, 2012].

Siegel, Larry J. 2011. Essentials of Criminal Justice, 7th Edition. Belmont, CA: Wadsworth.

Stark, Ronald B. 2008. Reporting of Employee Malfeasance, Travel Advances. *USG Memorandum*. Atlanta, GA: USG Office of Internal Audit.

The IIA. 2013. Certified Internal Auditor. https://na.theiia.org/certification/cia-certification/pages/cia-certification.aspx [Accessed February 2, 2013].

----- 2011. Number of Certified Internal Auditors Reaches 100K. http://www.prweb.com/releases/2011/4/prweb8260999.htm [Accessed February 17, 2013].

The Institute of Internal Auditors. 1997. *Standards for the Professional Practice of Internal Auditing*. Altamonte Springs, FL: The Institute of Internal Auditors.

University System of Georgia. 2010a. Section 16.4 Malfeasance Reporting, Business Procedures Manual. http://www.usg.edu/business_procedures_manual/section16/C1526 [Accessed October 10, 2012].

----- 2010b. Section 3.3 Purchasing Cards, Business Procedures Manual. http://www.usg.edu/business_procedures_manual/section3/C1127 [Accessed October 10, 2012].

USG Office of Internal Audit. 2008. *Review of USG Purchasing Card Administration and FY 2007 Transaction Review, Final Report*. Atlanta: University System of Georgia Office of Internal Audit.

WSB TV. 2011. Another Georgia Tech Professor Under Criminal Investigation. http://www.wsbtv.com/news/news/another-georgia-tech-professor-under-criminal-inve/nJbZh/ [Accessed February 20, 2013].

WSB TV. 2008. More Tech Employees Arrested, Charged With Credit Card Fraud. http://www.wsbtv.com/news/news/more-tech-employees-arrested-charged-with-credit-c/nFCXM/ [Accessed January 31, 2012].

Appendices

Appendix A: Interview Questions for Georgia Tech's Chief Audit Executive

1. Was your internal auditing department affected by the passage of Georgia 2008 House Bill 1113 (HB 1113) and subsequent USG policy change in regards to reporting suspected employee malfeasance?
   If yes, please describe the immediate and long term effects on your department.

2. Has HB 1113 and subsequent USG policy changes on reporting suspected employee malfeasance had an effect on your department's budgetary planning and funding?
   If yes, please describe the effects on budgetary planning and funding.

3. Has HB 1113 and subsequent USG policy changes on reporting suspected employee malfeasance had an effect on your department's staffing?
   If yes, please describe the effects on staffing.

4. Has HB 1113 and subsequent USG policy changes on reporting suspected employee malfeasance had an effect on the training /certifications your staff has received?
   If yes, please describe the effects on training.

5. Has HB 1113 and subsequent USG policy changes on reporting suspected employee malfeasance had an effect on the tools or technology your department utilizes?
   If yes, please describe the effects on departmental tools or technology.

6. Has HB 1113 and subsequent USG policy changes on reporting suspected employee malfeasance had an effect with your department's campus communication efforts?
   If yes, please describe the effects on campus communication.

7. Has HB 1113 and subsequent USG policy changes on reporting suspected employee malfeasance raised awareness of employee malfeasance on your campus?
   If yes, please describe the manner in which awareness has been raised.

Appendix B: USG Memorandum of Reporting Employee Malfeasance

BOARD OF REGENTS OF
THE UNIVERSITY SYSTEM OF GEORGIA

OFFICE OF INTERNAL AUDIT
270 WASHINGTON STREET, S.W.
ATLANTA, GEORGIA 30334

(404) 657-2237 - PHONE
(404) 463-0999 - FAX
RON.STARK@USG.EDU

MEMORANDUM

Date: May 6, 2008

To: Presidents, University System of Georgia

To: Chief Business Officers, University System of Georgia

To: Chief Academic Officers, University System of Georgia

CC: Erroll B. Davis, Jr., Chancellor

CC: Chancellor's Cabinet

From: Ronald B. Stark, Chief Audit Officer & Associate Vice Chancellor

Re: Reporting of Employee Malfeasance, Travel Advances – Interim Update

The recent P-Card audit and associated alleged fraud has resulted in a requirement for more formalized reporting of alleged employee malfeasance to both my office and to the Attorney General's Office. Additionally, the General Assembly passed House Bill (HB) 1113 on the last day of the Session. HB 1113 also addressed aspects of P-Card program management, penalties associated with P-Card misuse, and the penalties associated with misuse of travel advances and fraudulent requests to the state for reimbursement.

The purpose of this memo is (1) to outline a new requirement pertaining to reporting of employee malfeasance, and (2) to make each USG institution aware of the changes introduced by HB 1113. The requirements outlined below will be reflected in future revisions of the USG Business Procedures Manual (BPM).

Reporting of Employee Malfeasance – Effective immediately, all USG institutions are expected to report all suspected employee malfeasance to my office. Currently, the USG BPM Section 16.4.5 requires institutions to report malfeasance only when it has been "determined that a 'high likelihood' of impropriety greater than $1000 has occurred." However, the Attorney General's (AG's) Office has since requested that they be provided an opportunity to review all cases of alleged employee malfeasance. The AG's Office has also requested that my office be responsible for coordinating the collection of this information. It is expected that the majority of cases will still be handled by local district attorneys.

Employee malfeasance generally includes instances of embezzlement, misappropriation, alteration or falsification of documents, false claims, theft of any asset, inappropriate use of computer systems to include hacking and software piracy, bribery or kickback, etc. Note that this requirement applies only to employee malfeasance. Actions by students or outside parties do not fall within the scope of this requirement.

Reports of employee malfeasance should include the following components:

- The institution's name, the institution point of contact to include telephone and email;
- Description of the incident to include incident date and time, location, improper activity, estimated loss to the institution, etc.;
- Known suspect information to include employee name, title, employment status (administrative leave, pending termination, etc.), etc.; and,
- Current case status to include law enforcement involvement and the results of any internal investigation.

Reports should be clearly marked as confidential. It is expected that institutions will report suspected employee malfeasance once an initial determination has been made that employee malfeasance was likely. Institutions are not authorized to negotiate a promise to not report employee malfeasance in return for the employee's resignation, restitution, etc. The decision not to prosecute rests with the Attorney General's Office.

Please submit your reports to my office via email to Ron Stark at ron.stark@usg.edu and to the USG Compliance Officer John Fuchko at john.fuchko@usg.edu. Alternatively, reports may be sent by hard copy ATTN: Mr. Ron Stark and Mr. John Fuchko at the Office of Internal Audit, University System of Georgia, 270 Washington Street, Atlanta, GA 30334.

HB 1113 – HB 1113 introduces multiple new requirements pertaining to both P-Card program administration and the use of travel advances and reimbursement requests. This legislation has not yet been signed by the Governor. However, it is expected that the Governor will sign this legislation. Without attempting to address every point made in the legislation, I would like to highlight the following points:

- Criminal penalties associated with P-Card misuse have been significantly increased;

- Both P-Card cardholders and supervisors may be criminally prosecuted for P-Card misuse – a supervisor that "knowingly intentionally, willfully, wantonly, or recklessly allows or who conspires with an employee who is issued a purchasing card to violate subsection (c) of this Code section shall be subject to immediate termination of employment and criminal prosecution."

- P-Card misuse that may result in civil and criminal penalties includes:

    - Uses a purchasing card for personal gain;

    - Purchases items on such purchasing card that are not authorized for purchase by such employee;

    - Purchases items in violation of this Code section; or

- Retains for such employee's personal use a rebate or refund from a vendor, bank, or other financial institution for a purchase or the use of a purchasing card.

This definition of misuse could conceivably include purchase categorized as "policy violations" in addition to the more obvious misuse through personal gain.

- The legislation also specifically addresses travel advances and reimbursement requests as follows:

  - It shall be unlawful for any person to use any travel advance received from public funds, for nongovernmental purposes or to submit or approve, knowingly or through willful and wanton neglect, a fraudulent request to the state for reimbursement of expenses.

The penalties associated with violation of this law ranges from a misdemeanor of a high and aggravated nature for aggregate amounts less than $500 to a felony for aggregate amounts of $500 or greater. The restitution requirements, fines, and prison time associated with these crimes can be found in HB 1113.

We recommend that institutions take the following steps to prepare for implementation of HB 1113:

1. Continue to implement the recommendations outlined in the February 28, 2008, consolidated P-Card report.

2. Be prepared to implement new P-Card policies once issued by the Georgia Department of Administrative Services (DOAS) and the USO. Note that a draft policy that addresses the HB 1113 requirements pertaining to P-Cards has already been drafted by my office and has been reviewed by DOAS, the Office of Planning and Budget, the State Accounting Office, and the State Auditor's Office.

3. Update internal procedures and documents to clearly communicate the various penalties associated with misuse of travel advances and the submittal of fraudulent requests for reimbursement.

4. Review current travel advances outstanding to employees and immediately collect outstanding travel advances. Note that institutions are not authorized to negotiate "payment plans" with employees. Rather, employees are expected to immediately return outstanding travel advances. Outstanding travel advances are those funds that must be accounted for and/or returned to the institution as outlined in BPM Sections 4.9.4 through 4.9.9.

Please do not hesitate to contact my office with any questions or concerns pertaining to the above issues.

Appendix C: GT-DIA QAR Report, Executive Summary

Georgia Institute of Technology - External Quality Assessment

Executive Summary

The Georgia Institute of Technology (GT) Department of Internal Audit (DIA) was established in 1978 by Dr. J. M. Petit, then President of the Institute. Dr. Petit in a memorandum to the campus on March 15, 1978, explained the establishment of the internal audit operation. DIA is staffed with competent professionals, produces quality written reports and is highly respected within the University of Georgia System (USG) and GT management. Its conformance with IIA *Standards* earns the highest overall rating, while certain improvement opportunities are noted.

GT DIA is known as the 'go to' internal audit operation among its higher education peers. This office is seen as a leader in Information Technology (IT), forensic, PCard, and departmental auditing. Internal Audit has also been a catalyst for the establishment and upcoming launch of the Institute's control self assessment.

Successful deployment of the hotline software by the DIA has resulted in a high number of investigations undertaken by DIA. This has placed DIA in a reactive instead of proactive mode. The skills of the DIA staff are well suited to the investigative activities they undertake and this role is of great value to GT. Recently, a Forensic Audit unit was established in DIA. We note, however, that these activities have undermined the full cadre of services DIA may provide GT. Currently, Institute perception of DIA is of being exclusively campus investigators instead of the more helpful reputation of assurance specialists and consultants. During the upcoming year, we believe the DIA will be recognized for their assurance and consulting activities because of the strategic vision of the Director/Chief Audit Executive (CAE) of the DIA. We have confidence this will the preferred bring balance to the assurance, investigative, and consulting activities offered by the DIA. Conducting client satisfaction surveys would provide helpful feedback toward this goal and also help DIA continuously assess its quality of services provided.

While we recognize that there are many different organizational models for internal audit operations to ensure internal auditors are in a position where they are sufficiently independent, we found day-to-day business processes are coordinated through an Associate Vice President. The DIA Director/CAE does appear to have immediate access to the President. While electronic working papers make for efficient work; we have noted some opportunities to enhance these working papers and the process.

****

Appendix III is a maturity model developed by the IIA that is designed for commercial enterprises. It is presented for informational purposes only. There are other models perhaps more suited to the University's circumstances that could be used as a basis for discussion with senior management and the Committee on Internal Audit, Risk and Compliance about the Internal Audit Program's current and desired future state.